TITLE:

Quadratic Frobenius test and cyclotomic polynomials(Computer Algebra - Design of Algorithms, Implementations and Applications)

AUTHOR(S):

篠原, 直行

CITATION:

篠原, 直行. Quadratic Frobenius test and cyclotomic polynomials(Computer Algebra - Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2007, 1568: 27-33

ISSUE DATE:

2007-09

URL:

http://hdl.handle.net/2433/81232

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
第1568巻 2007年 27-33

Quadratic Frobenius test and cyclotomic polynomials

篠原 直行
NAOYUKI SHINOHARA*
CREST JST / 立教大学
CREST JST / RIKKYO UNIV.

Abstract

Frobenius test は与えられた整数が合成数であるか否かを判定するアルゴリズムであるが, まれに合成数を合成数ではないと判定する場合がある. そのような合成数は Frobenius 擬素数と呼ばれ, それは通常, 整数の組 (a,b) の影響をうける. 本稿では, 与えられた奇合成数 n がパラメータ (a,b) に対して Frobenius 擬素数となるときの, n と (a,b) の関係についての結果と背景について述べる.

1 序論

素数判定とは, 与えられた整数 n が合成数であるか "確率的な素数" であるかを判定するアルゴリズムである. "確率的な素数" とは, 素数または素数判定をパスした合成数である. つまり, 素数判定テストにおいては合成数でありながら合成数と判定されない数が存在し, それは擬素数と呼ばれる. このような合成数が存在する理由は, 素数判定は「n が素数ならば, 条件 S が成り立つ」という定理の対偶に基づくアルゴリズムだからである. もちろん, 合成数が素数判定をパスする確率が低いほどよいアルゴリズムと言える.

一方, 素数証明と呼ばれるアルゴリズムは, 素数と判定された数が必ず素数であるという特徴を持つ. 当然ながら, この意味において素数証明は素数判定より上位のアルゴリズムと言える. ただ, 実用的な, つまり与えられた整数を n としたときに計算量が $\mathcal{O}((\log n)^5)$ より小さいアルゴリズムは現在知られていない.

多くの種類の素数判定の計算量は $\mathcal{O}((\log n)^3)$ であるため, ある素数判定にいくつかの数学的な条件を付け加えることで実用的な素数証明を構築することは効果的である考えられる. その例として, Felmat の小定理を応用した Miller-Rabin test に, E.R.H. が成り立つことを前提として, ある条件を組み合わせたアルゴリズムがあげられる. ただ, E.R.H. が証明されていないため, このアルゴリズムは正確には素数証明とは認められていない. そこで, 他の素数判定で同様のことを考えてみる.

General Frobenius test [1] は J. Grantham によって提案された素数判定であり, その特別な場合である Quadratic Frobenius test から素数証明を構築することを考える. 本稿では Quadratic Frobenius test を単に Frobenius test と呼ぶことにして, その説明から話をはじめる.

Frobenius test とは, 次の 定理 1.1 [1] の対偶を用いた素数判定である.

定理 1.1 a,b は $\Delta = a^2 - 4b \neq 0$ を満たす整数とする. また素数 n は $\gcd(n, 2b\Delta) = 1$ を満たすものとす

*shnhr@tvs.rikkyo.ne.jp

る．このとき次の合同式が成り立つ．

$$x^n \equiv \begin{cases} a-x \pmod{(x^2-ax+b,n)}, & ((\frac{\Delta}{n})=-1 \text{ のとき}), \\ x \pmod{(x^2-ax+b,n)}, & ((\frac{\Delta}{n})=1 \text{ のとき}) \end{cases} \tag{1}$$

ここで，n が $\gcd(n,2b\Delta)=1$ なる合成数でありながら式 (1) を満たすものが存在する．それを (a,b) に対する Frobenius 擬素数とよび，$fpsp(a,b)$ とかく．

Frobenius test から素数証明を構築する上で，$fpsp(a,b)$ なる合成数とパラメータ (a,b) の関係を明らかにすることは非常に重要である．(これは Miller-Rabin test と E.R.H. を組み合わせたアルゴリズムを構築する手法と同じ方針である.) 本稿では $fpsp(a,b)$ となる奇合成数とそのときの整数の組 (a,b) との関係を，素冪環における円分多項式の “因子” の性質から考察した．(ただ，素冪環 $\mathbf{Z}/p^e\mathbf{Z}$ は $e>1$ のときは整域ではないため，素冪環での多項式の “既約性” や “因子” の取り扱いには一般には注意が必要である．しかし，本稿で取り扱う内容においては通常の規約性や因子と同様に考えても問題はない.)

Frobenius test による n の判定結果は $(\mathbf{Z}/n\mathbf{Z})[x]/(x^2-ax+b)$ における x の位数に左右される．当然ながら x は有限位数をもちそれを M とするとし，第 m 円分多項式を $\Phi_m(x)$ と書くこととすれば，

$$x^M-1=\prod_{m \mid M}\Phi_m(x) \equiv 0 \pmod{(x^2-ax+b,p^e)}$$

が n の任意の素冪因子 p^e に対して成り立つ．つまり，x^2-ax+b は $\mathbf{Z}/p^e\mathbf{Z}$ において x^M-1 の “因子” であると考えられ，さらに x^M-1 が円分多項式の積でかけることに注目したわけである．

以後は考えやすくするため次の補題 1.2 の条件 (2) に注目する．

補題 1.2. a,b は $\Delta=a^2-4b\neq 0$ を満たす整数とする．このとき $\gcd(n,2b\Delta)=1$ なる合成数 n が $fpsp(a,b)$ であることと以下の合同式が成り立つことは同値である．

$$x^{n-(\frac{\Delta}{n})} \equiv \begin{cases} b \pmod{(x^2-ax+b,n)} & ((\frac{\Delta}{n})=-1 \text{ のとき}), \\ 1 \pmod{(x^2-ax+b,n)} & ((\frac{\Delta}{n})=1 \text{ のとき}). \end{cases} \tag{2}$$

2 Frobenius 擬素数と ICF

円分多項式の性質を話す前に，この章で Frobenius 擬素数の分類と，与えられた (a,b) に対して奇合成数 n が各種の Frobenius 擬素数になるときの同値条件 $(ICF1)$ から $(ICF5)$ を紹介する．

$1\leq a,b\leq 10$ かつ $\Delta=a^2-4b$ が平方数にならない組 (a,b) それぞれに対して，区間 $[50000,10^8+50000]$ 内のすべての奇合成数に対して Frobenius test を行った．その結果，$fpsp(a,b)$ の個数が 1000 を超える (a,b) の特徴がわかった．それは，$b=1$ となる場合の (a,b) か Lucas sequence が退化数列となる場合の (a,b) である．後者の原因は Lucas test の性質によるものである．さらに，$b=-1$ となる場合の同様の実

験結果では, $fpsp(a,-1)$ の個数は 500 個を超えることがわかった. これらの (a,b) に対する Frobenius 擬素数の個数は, 他の (a,b) に対して非常に大きなものである. またこれらの実験結果から, $(\frac{\Delta}{n}) = -1$ かつ $b \neq \pm 1$ なる $n = fpsp(a,b)$ は 291409 のみであることは興味深い事実である.

これらの結果から, $b = \pm 1$ と $(\frac{\Delta}{n})$ の値に注意して, Frobenius 擬素数を以下の五つに分類した. 各種の Frobenius 擬素数は互いに背反である.

定義 2.1 (Frobenius pseudoprime of the first type). n は $fpsp(a,b)$ で, さらに n の全ての素因子 p に対して $(\frac{\Delta}{p}) = 1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the first type* とよび, さらに $fpsp1(a,b)$ とかく.

定義 2.2 (Frobenius pseudoprime of the second type). n は $fpsp(a,b)$ で, さらに n の少なくとも 1 つの素因子 p に対して $(\frac{\Delta}{p}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the second type* とよび, さらに $fpsp2(a,b)$ とかく.

定義 2.3 (Frobenius pseudoprime of the third type). n は $fpsp(a,b)$ で, さらに $b \equiv 1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the third type* とよび, さらに $fpsp3(a,b)$ とかく.

定義 2.4 (Frobenius pseudoprime of the fourth type). n は $fpsp(a,b)$ で, さらに $b \equiv -1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the fourth type* とよび, さらに $fpsp4(a,b)$ とかく.

定義 2.5 (Frobenius pseudoprime of the fifth type). n は $fpsp(a,b)$ で, さらに $b \not\equiv \pm 1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the fifth type* とよび, さらに $fpsp5(a,b)$ とかく.

知りたいのは, 与えられた奇合成数 n が $fpsp(a,b)$ となる (n,a,b) の組の条件である. そのような条件を以下のように定義した.

定義 2.6 (Inefficasious conditions of Frobenius test (ICF)). いくつかの条件を満たす全ての数が *Frobenius* 擬素数となるものが存在し, それらの条件を "Inefficacious Conditions of Frobenius test (ICF)" とよぶ.

例えば, $(a,b) = (1,1)$ かつ合成数 n が $\gcd(n,6) = 1$ を満たすという条件は ICF である. なぜならば, その条件の下では n が $fpsp(1,1)$ だからである.

ここでは, 各タイプの Frobenius 擬素数の同値条件をそれぞれ, $ICF1$ から $ICF5$ までで与える. ただ, その前にいくつか注意点と定義について述べる.

定義 2.7. $g(x)$ と $h(x)$ はモニックな整数係数多項式であるとする. $h(x) \equiv 0 \pmod{(p^e, g(x))}$ であるとき, "$g(x)$ は $\mathbf{Z}/p^e\mathbf{Z}$ 上で $h(x)$ をわりきる" といい, $g(x) \mid_{p^e} h(x)$ とかく.

式 (2) より, n が $fpsp(a,b)$ であるならば, ある自然数 M が存在して $x^M \equiv 1 \pmod{(n, x^2 - ax + b)}$ が成り立つ. 従って, n の最大素冪因子 p^e において, $x^2 - ax + b$ は $\mathbf{Z}/p^e\mathbf{Z}$ 上での $x^M - 1$ の "因子" と考えることができる. "因子" と書いたのは, $e > 1$ である場合 $\mathbf{Z}/p^e\mathbf{Z}$ は整域でないからである. しかし, 第 3 節で述べるが, $p \nmid M$ の場合に $x^M - 1$ の "因子" は自然に定義でき, また $\mathbf{Z}/p^e\mathbf{Z}$ 上の既約性についてもモニックなものに限れば自然に定義できる. 円分多項式が素冪環上でどのように因数分解されるかを調べることによって, 奇合成数 n が (a,b) に対して各種の Frobenius 擬素数になるときの以下のような同値条件, $ICF1$ から $ICF5$ を得ることができた.

定義 2.8 (ICF of the first type ($ICF1$)). a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF1$"* とよぶ.
$(ICF1-1)$ 各 $i\in[1,k]$ に対して, $f(x)\equiv(x-c_{i,1})(x-c_{i,2})\pmod{p_i^{e_i}}$ かつ $c_{i,1}\not\equiv c_{i,2}\pmod{p_i^{e_i}}$ で,

$$x-c_{i,1}\mid_{p_i^{e_i}}\Phi_{m_i}(x),\ x-c_{i,2}\mid_{p_i^{e_i}}\Phi_{m_i'}(x)$$

をみたす自然数 m_i,m_i' が存在する.
$(ICF1-2)$ $m=lcm(m_1,m_1',...,m_k,m_k')$ に対して $n\equiv 1\pmod m$.

奇合成数 n が $fpsp1(a,b)$ であることと, (n,a,b) に対して $ICF1$ が成り立つことは同値である.

定義 2.9 (ICF of the second type ($ICF2$)). a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF2$"* とよぶ.
$(ICF2-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbf{Z}/p_i^{e_i}\mathbf{Z}$ 上既約で, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる m_j が存在する.
$(ICF2-2)$ $\sum_{i=1}^{k}e_i\equiv 0\pmod 2$ が成り立つ.
$(ICF2-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_{i,1})(x-c_{i,2})\pmod{p_i^{e_i}}$ かつ $c_{i,1}\not\equiv c_{i,2}\pmod{p_i^{e_i}}$ で,

$$x-c_{i,1}\mid_{p_i^{e_i}}\Phi_{m_i}(x),\ x-c_{i,2}\mid_{p_i^{e_i}}\Phi_{m_i'}(x)$$

なる自然数 m_i,m_i' が存在する.
$(ICF2-4)$ $m=lcm(m_1,...,m_k,m_{k+1},m_{k+1}',...,m_{k+\ell},m_{k+\ell}')$ に対して $n\equiv 1\pmod m$ が成り立つ.

奇合成数 n が $fpsp2(a,b)$ であることと, (n,a,b) に対して $ICF2$ が成り立つことは同値である.

定義 2.10 (ICF of the third type ($ICF3$)). a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF3$"* とよぶ.
$(ICF3-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbf{Z}/p_i^{e_i}\mathbf{Z}$ 上既約で, さらに $p_i\equiv -1\pmod{m_i}$, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 $m_i>2$ が存在する.
$(ICF3-2)$ $\sum_{i=1}^{k}e_i\equiv 1\pmod 2$ が成り立つ.
$(ICF3-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x-c_i^{-1})\pmod{p_i^{e_i}}$ で, さらに $x-c_i\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 $m_i>2$ が存在する.
$(ICF3-4)$ $m=lcm(m_1,...,m_{k+\ell})$ に対して $n\equiv -1\pmod m$ が成り立つ.

奇合成数 n が $fpsp3(a,b)$ であることと, (n,a,b) に対して $ICF3$ が成り立つことは同値である.

定義 2.11 (ICF of the fourth ($ICF4$)). a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF4$"* とよぶ.
$(ICF4-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbf{Z}/p_i^{e_i}\mathbf{Z}$ 上既約で, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ と

$$s_i\geq 2,\ p_i\equiv 2^{s_i-1}r_i-1\pmod m \text{ かつ } m_i\neq 4 \tag{3}$$

を満たす自然数 $m_i=2^{s_i}r_i$ が存在する. ただし r_i は奇数とする.
$(ICF4-2)$ $\sum_{i=1}^{k}e_i\equiv 1\pmod 2$ が成り立つ.
$(ICF4-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x+c_i^{-1})\pmod{p_i^{e_i}}$ で, さらに $x-c_i\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 m_i が存在する.
$(ICF4-4)$ $m=lcm(m_1,...,m_{k+\ell})$ に対して, $n\not\equiv -1\pmod m$, $2(n+1)\equiv 0\pmod m$ が成り立つ.

奇合成数 n が $fpsp4(a,b)$ であることと, (n,a,b) に対して $ICF4$ が成り立つことは同値である.

定義 2.12 (ICF of the fifth type ($ICF5$)). a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF5$"* とよぶ.
($ICF5-1$) 各 $i\in[1,k]$ に対して, $m_I \mid \gcd(p_in-1,p_i^2-1)$, $m_i\nmid p_i-1$ なる自然数 m_i が存在する.
($ICF5-2$) 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上既約で, さらに $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ が成り立つ.
($ICF5-3$) $\sum_{i=1}^{k}e_i\equiv 1 \pmod 2$ が成り立つ.
($ICF5-4$) 各 $i\in[k+1,k+\ell]$ に対して, $m_i\mid\gcd(n^2-1,p_i-1)$, $m_i\nmid n-1$ をみたす自然数 m_i が存在する.
($ICF5-5$) 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x-c_i^n) \pmod{p_i^{e_i}}$ となり, さらに $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる整数 m_i が存在する.
($ICF5-6$) $b\not\equiv\pm1 \pmod n$ が成り立つ.

奇合成数 n が $fpsp5(a,b)$ であることと, (n,a,b) に対して $ICF5$ が成り立つことは同値である.

3 気素数冪環上での第 m 円分多項式 $\Phi_m(x)$ の因子

この章では $ICF1$ から $ICF5$ までを得るために必要な円分多項式の性質, 素冪環 $\mathbb{Z}/p^e\mathbb{Z}$ 上で円分多項式がどのように "因数分解" されるかについて述べる. $\mathbb{Z}/p^e\mathbb{Z}$ における $\Phi_m(x)$ の "因子" は, Hensel の補題 によって, $\mathbb{F}_p$ 上での因子からリフトアップして得られる.
まず, 一般によく知られている事実として補題 3.1 をあげておく. square-free は Hensel の補題 を用いる上で重要な意味を持つ.

補題 3.1. p が m を割り切らないことと, $\Phi_m(x)$ が $\mathbb{F}_p$ 上 *square-free* であることは同値である.

以後, p は与えられた奇合成数 n の素因子であるとし, さらに m は自然数で p で割り切れないものとする.

次の補題 3.2 は, $\mathbb{Z}$ 上では既約である円分多項式 $\Phi_m(x)$ が素体上 $\mathbb{F}_p$ 上で square-free に因数分解されるときの, m と p の関係と因子の次数にかかわる基本的な事実である.

補題 3.2. $1\le j\le k-1$ なるすべての j に対して

$$m\mid p^k-1\ ,\ m\nmid p^j-1 \iff \Phi_m(x)\equiv\prod_{i=1}^{\varphi(m)}g_i(x) \pmod p.$$

ただし $g_i(x)$ は次数 k の $\mathbb{F}_p$ 上既約な整数係数多項式で, φ は *Euler's totient functon* とする.

$e>1$ のとき $\mathbb{Z}/p^e\mathbb{Z}$ は整域ではないが, モニックな多項式については既約性が以下のように自然に定義できる.

定義 3.3. $g(x)$ をモニックな整数係数多項式であるとする. このとき,

$$g(x)\equiv s(x)t(x) \pmod{p^e} \text{ and } 0<\deg s<\deg g.$$

なる整数係数多項式 $s(x),t(x)$ が存在しないとき, *"$g(x)$ は $\mathbb{Z}/p^e\mathbb{Z}$ 上既約である"* という.

補題 3.1, 補題 3.2 と Hensel の補題 から補題 3.4 を得る.

補題 3.4. $1 \leq j \leq k-1$ なるすべての j に対して

$$m \mid p^k - 1\ ,\ m \nmid p^j - 1 \iff \Phi_m(x) \equiv \prod_{i=1}^{\varphi(m)} g_{e,i}(x) \pmod{p^e}.$$

ただし, $g_{e,i}(x)$ は次数 k の $(\mathbf{Z}/p^e\mathbf{Z})$ 上既約な整数係数多項式であるものとする. さらに, 全ての i と $1 \leq e' \leq e-1$ なる全ての e' に対して $g_{e'+1,i}(x) \equiv g_{e',i}(x) \pmod{p^{e'}}$ であるものとする.

$\mathbf{Z}/p^e\mathbf{Z}$ 上の $\Phi_m(x)$ の "因子" については, p が m を割り切らなければ自然に定義できることを補題 3.4 が示している. つまり, $\mathbf{Z}/p^e\mathbf{Z}$ 上の $\Phi_m(x)$ の "因子" は $\mathbf{F}_p$ 上の因子をリフトアップしたものである.

補題 3.1 と補題 3.4 より, 以下の系を得る. 以後, これらの系をもとに話を進めていく.

系 3.5 $p \equiv 1 \pmod{m}$ であることと, $\Phi_m(x)$ が $\mathbf{Z}/p^e\mathbf{Z}$ 上で一次の多項式に因数分解され, さらに *square-free* であることは同値である.

系 3.6 $p^2 \equiv 1 \pmod{m}$, $p \not\equiv 1 \pmod{m}$ であることと, $\Phi_m(x)$ が $\mathbf{Z}/p^e\mathbf{Z}$ 上で二次の既約多項式に因数分解され, さらに *square-free* であることは同値である.

ここでは, *fpsp3* と *fpsp4*, つまり *ICF3* と *ICF4* を得るために必要となる, $x^2 - ax \pm 1$ が素冪環上で $x^m - 1$ を割り切る場合について述べる. 二次多項式が既約である場合の補題 3.8 と補題 3.10 は, 次の補題 3.7 によるものである.

補題 3.7. $g_e(x) = x^2 - a_e x + b_e$ は $\Phi_m(x)$ の $\mathbf{Z}/p^e\mathbf{Z}$ 上既約な因子であるものとする. このとき次が成り立つ.

$$x^p \equiv a_e - x \pmod{(p^e, g_e(x))},\ (a_e - x)^p \equiv x \pmod{(p^e, g_e(x))}.$$

ICF3, つまり定数項 b が $b \equiv 1 \pmod{p^e}$ となる場合に必要な補題から紹介する.

補題 3.8. $m > 2$ かつ $p \equiv -1 \pmod{m}$ であることと

$$\Phi_m(x) \equiv \prod_{i=1}^{\varphi(m)} g_{e,i}(x) \equiv \prod (x^2 - a_{e,i}x + 1) \pmod{p^e}$$

であることは同値である. ただし, $g_{e,i}(x)$ は $\mathbf{Z}/p^e\mathbf{Z}$ 上既約であるとする.

二次多項式が可約な場合は $(x-c)(x-c^{-1}) \pmod{p^e}$ となる整数 c が存在しなくてはならない.

補題 3.9. $p \equiv 1 \pmod{m}$ であるとき, $x - c \mid_{p^e} \Phi_m(x)$ なる任意の $c \in (\mathbf{Z}/p^e\mathbf{Z})^*$ に対して $x - c^{-1} \mid_{p^e} \Phi_m(x)$ が成り立つ.

ICF4, つまり定数項 b が $b \equiv -1 \pmod{p^e}$ となる場合に必要な補題は以下のとおりである.

補題 3.10. 奇数 r と自然数 s に対して, $m = 2^s r$ とかけるものとする. このとき *(3)* が成り立つことと

$$\Phi_m(x) \equiv \prod_{i=1}^{\varphi(m)} g_{e,i}(x) \equiv \prod (x^2 - a_{e,i}x - 1) \pmod{p^e}$$

であることは同値である. ただし, $g_{e,i}(x)$ は $\mathbf{Z}/p^e\mathbf{Z}$ 上既約であるとする.

今度は x^M-1 が $x^2-ax\pm1$ なる $\mathbb{Z}/p^e\mathbb{Z}$ 上可約な因子持つ場合について述べる. 具体的には, $x^2-ax\pm1\equiv(x-c)(x\pm c^{-1})\pmod{p^e}$ とできて, $m\mid M$ なる自然数 m に対して $x-c\mid_{p^e}\Phi_m(x)$ ならば $x\pm c^{-1}\mid_{p^e}\Phi_d(x)$ なる d は何かについてである.

二次多項式が可約な場合は $(x-c)(x+c^{-1})\pmod{p^e}$ となる整数 c が存在しなくてはならない.

補題 3.11. 自然数 m が奇数 r と自然数 $s>1$ に対して $m=2^sr$ とかけて, $p\equiv1\pmod m$ が成り立つとき, $x-c\mid_{p^e}\Phi_m(x)$ であることと $x+c^{-1}\mid_{p^e}\Phi_m(x)$ であることは同値である.

補題 3.12. $p\equiv1\pmod m$ であるとき, $x-c\mid_{p^e}\Phi_m(x)$ であることと $x+c^{-1}\mid_{p^e}\Phi_{2m}(x)$ であることは同値である.

4 まとめ

我々が目標としたのは $fpsp(a,b)$ と (a,b) の関係を明らかにすることであり, それは本稿で述べた $ICF1$ から $ICF5$ で示したことである.

さらに, 本稿で紹介した各種の ICF を基に, 奇合成数 n が各種の Frobenius 擬素数になるような (a,b) が存在するかどうかを判定し, 存在する場合はそのような (a,b) を計算するアルゴリズムを構築することができる. そのアルゴリズムのステップは各 ICF の条件に基づいて, (i) n とその素因子 p_i の関係から m_i を決定し, (ii) 円分多項式 $\Phi_{m_i}(x)$ を計算, (iii) $\Phi_{m_i}(x)$ を素体 $\mathbb{F}_{p_i}$ で因数分解, (iv) Hensel's Lemma をつかって $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上の因子を計算, (v) 因子から得られた二次多項式 $f_i(x)=x^2-a_ix+b_i$ から中国式剰余定理を用いて, 各 i に対して $x^2-ax+b\equiv f_i(x)\pmod{p_i^{e_i}}$ なる (a,b) を計算する, の五つからなる.

今後の課題は Frobenius test から素数証明を構築することであるが, このことに関して J. Grantham によって与えられた非常に興味深い問題がある. "$fpsp5(-5,5)$ となるような合成数を発見しその因数分解を与えよ." $ICF5$ のさらなる解析からこの問題を解くことを試みたいと思う.

[1] R. Crandall and C. Pomerance. *Lucas pseudoprimes*, Pime Numbers (2001), 130-140.

[2] J. Grantham. *A probable prime test with high confidence*, J. Number Theory 72 (1998), 32-47.